CLAIMS

1. A method for enabling the rendering of digital content on a device, the method comprising:

transferring the content to the device;

obtaining a digital license corresponding to the content;

composing a sub-license corresponding to and based on the obtained license and transferring the composed sub-license to the device, to enable rendering of the content on the device only in accordance with the terms of the sub-license on the device.

2. The method of claim 1 further comprising, prior to composing the sub-license and transferring the composed sub-license to the device, checking the obtained license to determine that such license permits issuance of the sub-license to the device.

3. The method of claim 1 further comprising:

coupling the device to a computer;

placing the obtained license on the computer; and

transferring the composed sub-license from the computer to the device.

4. The method of claim 3 wherein transferring the content to the device comprises placing the content on the computer and then transferring the content from the computer to the device.

5. The method of claim 1 wherein the content is encrypted and decryptable according to a content key and wherein the license includes the content key encrypted into a form un-decryptable by the device, the composing of the sub-license comprising re-encrypting the content key into a form that is decryptable by the device and placing the re-encrypted content key in the sub-license.

6. The method of claim 5 wherein the license is issued to a computer having a public key (PU) and a private key (PR) corresponding to (PU), and wherein the content key in the license is encrypted according to (PU) (PU(content key)), the re-encrypting of the content key comprising:

obtaining (PU(content key)) from the license;

applying (PR) to (PU(content key)) to obtain the content key; and

encrypting the content key according to a secret acquirable by the device.

7. The method of claim 6 wherein encrypting the content key comprises encrypting the content key according to a secret comprising a symmetric key.

8. The method of claim 5 wherein the composing of the sub-license further comprises placing a rights description in the sub-license, the rights description describing rights conferred by the license, the device rendering the corresponding content only in accordance with the rights description.

9. The method of claim 5 wherein the composing of the sub-license further comprises placing indexing information in the sub-license, the indexing information identifying a secret to the device that the device employs to decrypt the encrypted content key.

10. The method of claim 5 wherein the composing of the sub-license further comprises placing a signature in the sub-license, the signature verifying the sub-license.

11. A method for rendering digital content on a device, the method comprising:

receiving the content onto the device, the content being encrypted and decryptable according to a content key;

receiving a digital license corresponding to the content onto the device, the license including the content key encrypted and decryptable according to a secret, the license also including indexing information identifying the secret to the device;

obtaining the indexing information in the license to identify the secret;

acquiring the secret based at least in part on the indexing information;

applying the secret to the encrypted content key to decrypt and obtain the content key; and

applying the obtained content key to the encrypted content to decrypt and obtain the content.

12. The method of claim 11 wherein the license includes a signature, the method further comprising verifying the license based on the signature thereof and the secret.

13. The method of claim 11 wherein the license includes a rights description describing rights conferred by the license, the method comprising rendering the corresponding content only in accordance with the rights description.

14. A method for composing a license for rendering digital content on a device, the content being encrypted and decryptable according to a content key, the device having an identifier, the method comprising:

deriving a secret by:

obtaining the device identifier;

acquiring a super-secret that is also acquirable by the device; and

applying the obtained device identifier and super-secret to a function to derive the secret:

(SECRET) = function (device identifier, (SUPER-SECRET));

encrypting the content key according to the derived secret such that the content key is decryptable according to the secret; and

placing the encrypted content key in the license.

15. The method of claim 14 wherein the content has a content ID, the method comprising deriving a secret by:

obtaining the content ID of the content;

obtaining the device identifier;

acquiring a super-secret that is also acquirable by the device; and

applying the obtained content ID, device identifier, and super-secret to a function to derive the secret:

(SECRET) = function (content ID, device identifier, (SUPER-SECRET)).

16. The method of claim 14 wherein the super-secret is identified by indexing information, the method further comprising placing the indexing information in the license, whereby the device may obtain the indexing information from the license and thereby identify the super-secret by way of the indexing information.

17. The method of claim 14 wherein acquiring the super-secret comprises:

obtaining a super-super-secret;

deciding on an indexing value j identifying a particular super-secret; and

applying the obtained super-super-secret and the indexing value j to a function to derive the super-secret identified by the indexing value j:

(SUPER-SECRET) = function ((SUPER-SUPER-SECRET), j),

the method further comprising placing the indexing value j in the license, whereby the device may obtain the indexing value j from the license and thereby identify the super-secret by way of the indexing value.

18. The method of claim 17 wherein acquiring the super-secret comprises:

obtaining a super-super-secret having an indexing value k;

deciding on an indexing value j identifying a particular super-secret; and

applying the obtained super-super-secret and the indexing values j, k to a function to derive the super-secret identified by the indexing value j:

(SUPER-SECRET) = function ((SUPER-SUPER-SECRET), j, k),

the method further comprising placing the indexing values j, k in the license, whereby the device may obtain the indexing values j, k from the license and thereby identify the super-secret by way of the indexing value.

19. A method for rendering digital content on a device, the content being encrypted and decryptable according to a content key, the content key being encrypted and decryptable according to a secret, the device having an identifier, the method comprising:

obtaining the encrypted content key from a digital license corresponding to the content;

deriving the secret by:

obtaining the device identifier;

acquiring a super-secret; and

applying the obtained device identifier and super-secret to a function to derive the secret:

(SECRET) = function (device identifier, (SUPER-SECRET));

decrypting the content key according to the derived secret;

decrypting the content according to the derived content key; and

rendering the decrypted content.

20. The method of claim 19 wherein the content has a content ID, the method comprising deriving a secret by:

obtaining the content ID of the content;

obtaining the device identifier;

acquiring a super-secret; and

applying the obtained content ID, device identifier, and super-secret to a function to derive the secret:

(SECRET) = function (content ID, device identifier, (SUPER-SECRET)).

21. The method of claim 19 wherein the super-secret is identified by indexing information in the license, the method further comprising obtaining the indexing information from the license and thereby identifying the super-secret by way of the indexing information.

22. The method of claim 19 wherein the super-secret is identified by an indexing value j, the indexing value j being located in the license, and wherein acquiring the super-secret comprises:

obtaining a super-super-secret;

obtaining the indexing value j from the license and thereby identifying the super-secret by way of the indexing value j; and

applying the obtained super-super-secret and the indexing value j to a function to derive the super-secret identified by the indexing value j:

(SUPER-SECRET) = function ((SUPER-SUPER-SECRET), j).

23. The method of claim 22 wherein the super-super-secret is identified by an indexing value k, the indexing value k being located in the license, and wherein acquiring the super-secret comprises:

obtaining the indexing value k from the license and thereby identifying the super-super-secret by way of the indexing value k

obtaining the super-super-secret having the indexing value k;

obtaining the indexing value j from the license and thereby identifying the super-secret by way of the indexing value j; and

applying the obtained super-super-secret having the indexing value k and the indexing values j, k to a function to derive the super-secret identified by the indexing value j:

(SUPER-SECRET) = function ((SUPER-SUPER-SECRET), j, k).

24. A computer-readable medium having computer-executable instructions thereon for rendering digital content on a device, the instructions comprising modules including:

a first module for transferring the content to the device;

a second module for obtaining a digital license corresponding to the content; and

a third module for composing a sub-license corresponding to and based on the obtained license and transferring the composed sub-license to the device; the content on the device being rendered only in accordance with the terms of the sub-license on the device.

25. The medium of claim 24 further comprising, a fourth module for, prior to composing the sub-license and transferring the composed sub-license to the device, checking the obtained license to determine that such license permits issuance of the sub-license to the device.

26. The medium of claim 24 wherein the device is coupled to a computer, the second module placing the obtained license on the computer and

the third module transferring the composed sub-license from the computer to the device.

27. The medium of claim 26 wherein the first module places the content on the computer and then transfers the content from the computer to the device.

28. The medium of claim 24 wherein the content is encrypted and decryptable according to a content key and wherein the license includes the content key encrypted into a form un-decryptable by the device, the third module composing the sub-license by re-encrypting the content key into a form that is decryptable by the device and placing the re-encrypted content key in the sub-license.

29. The medium of claim 28 wherein the license is issued to a computer having a public key (PU) and a private key (PR) corresponding to (PU), and wherein the content key in the license is encrypted according to (PU) (PU(content key)), the third module re-encrypting the content key by:

obtaining (PU(content key)) from the license;

applying (PR) to (PU(content key)) to obtain the content key; and

encrypting the content key according to a secret acquirable by the device.

30. The medium of claim 29 wherein the third module encrypts the content key according to a secret comprising a symmetric key.

31. The medium of claim 28 wherein the third module places a rights description in the sub-license, the rights description describing rights

conferred by the license, the device rendering the corresponding content only in accordance with the rights description.

32. The medium of claim 28 wherein the third module places indexing information in the sub-license, the indexing information identifying a secret to the device that the device employs to decrypt the encrypted content key.

33. The medium of claim 28 wherein the third module places a signature in the sub-license, the signature verifying the sub-license.

34. A computer-readable medium having computer-executable instructions thereon for rendering digital content on a device, the instructions comprising modules including:

a first module for receiving the content onto the device, the content being encrypted and decryptable according to a content key;

a second module for receiving a digital license corresponding to the content onto the device, the license including the content key encrypted and decryptable according to a secret, the license also including indexing information identifying the secret to the device;

a third module for obtaining the indexing information in the license to identify the secret;

a fourth module for acquiring the secret based at least in part on the indexing information;

a fifth module for applying the secret to the encrypted content key to decrypt and obtain the content key; and

a sixth module for applying the obtained content key to the encrypted content to decrypt and obtain the content.

35. The medium of claim 34 wherein the license includes a signature, the medium further comprising a seventh module for verifying the license based on the signature thereof and the secret.

36. The medium of claim 34 wherein the license includes a rights description describing rights conferred by the license, the medium further comprising a seventh module for rendering the corresponding content only in accordance with the rights description.

37. A computer-readable medium having computer-executable instructions thereon for composing a license for rendering digital content on a device, the content being encrypted and decryptable according to a content key, the device having an identifier, the instructions comprising modules including:

a first module for deriving a secret by:

obtaining the device identifier;

acquiring a super-secret that is also acquirable by the device; and

applying the obtained device identifier and super-secret to a function to derive the secret:

(SECRET) = function (device identifier, (SUPER-SECRET));

a second module for encrypting the content key according to the derived secret such that the content key is decryptable according to the secret; and

a third module for placing the encrypted content key in the license.

38. The medium of claim 37 wherein the content has a content ID, the first module deriving a secret by:

obtaining the content ID of the content;

obtaining the device identifier;

acquiring a super-secret that is also acquirable by the device; and

applying the obtained content ID, device identifier, and super-secret to a function to derive the secret:

(SECRET) = function (content ID, device identifier, (SUPER-SECRET)).

39. The medium of claim 37 wherein the super-secret is identified by indexing information, the medium further comprising a fourth module for placing the indexing information in the license, whereby the device may obtain the indexing information from the license and thereby identify the super-secret by way of the indexing information.

40. The medium of claim 37 wherein the first module acquires the super-secret by:

obtaining a super-super-secret;

deciding on an indexing value j identifying a particular super-secret; and

applying the obtained super-super-secret and the indexing value j to a function to derive the super-secret identified by the indexing value j:

(SUPER-SECRET) = function ((SUPER-SUPER-SECRET), j),

the medium further comprising a fourth module for placing the indexing value j in the license, whereby the device may obtain the indexing value j from the license and thereby identify the super-secret by way of the indexing value.

41. The medium of claim 40 wherein the first module acquires the super-secret by:

obtaining a super-super-secret having an indexing value k;

deciding on an indexing value j identifying a particular super-secret; and

applying the obtained super-super-secret and the indexing values j, k to a function to derive the super-secret identified by the indexing value j:

(SUPER-SECRET) = function ((SUPER-SUPER-SECRET), j, k),

the medium further comprising a fourth module for placing the indexing values j, k in the license, whereby the device may obtain the indexing values j, k from the license and thereby identify the super-secret by way of the indexing value.

42. A computer-readable medium having computer-executable instructions thereon for rendering digital content on a device, the content being encrypted and decryptable according to a content key, the content key being encrypted and decryptable according to a secret, the device having an identifier, the instructions comprising modules including:

a first module for obtaining the encrypted content key from a digital license corresponding to the content;

a second module for deriving the secret by:

obtaining the device identifier;

acquiring a super-secret; and

applying the obtained device identifier and super-secret to a function to derive the secret:

(SECRET) = function (device identifier, (SUPER-SECRET));

a third module for decrypting the content key according to the derived secret;

a fourth module for decrypting the content according to the derived content key; and

a fifth module for rendering the decrypted content.

43. The medium of claim 42 wherein the content has a content ID, the first module deriving a secret by:

obtaining the content ID of the content;

obtaining the device identifier;

acquiring a super-secret; and

applying the obtained content ID, device identifier, and super-secret to a function to derive the secret:

(SECRET) = function (content ID, device identifier, (SUPER-SECRET)).

44. The medium of claim 42 wherein the super-secret is identified by indexing information in the license, the method further comprising a sixth module for obtaining the indexing information from the license and thereby identifying the super-secret by way of the indexing information.

45. The method of claim 42 wherein the super-secret is identified by an indexing value j, the indexing value j being located in the license, and wherein the first module acquires the super-secret by:

obtaining a super-super-secret;

obtaining the indexing value j from the license and thereby identifying the super-secret by way of the indexing value j; and

applying the obtained super-super-secret and the indexing value j to a function to derive the super-secret identified by the indexing value j:

(SUPER-SECRET) = function ((SUPER-SUPER-SECRET), j).

46. The method of claim 45 wherein the super-super-secret is identified by an indexing value k, the indexing value k being located in the license, and wherein the first module acquires the super-secret by:

obtaining the indexing value k from the license and thereby identifying the super-super-secret by way of the indexing value k

obtaining the super-super-secret having the indexing value k;

obtaining the indexing value j from the license and thereby identifying the super-secret by way of the indexing value j; and

applying the obtained super-super-secret having the indexing value k and the indexing values j, k to a function to derive the super-secret identified by the indexing value j:

(SUPER-SECRET) = function ((SUPER-SUPER-SECRET), j, k).